CLAIMS

What is claimed is:

5   1.   A method for preventing bridge loops in a network
topology, comprising:
        monitoring an intra-hub communication path of a network
hub to detect a first data unit on said intra-hub
communication path having a destination address matching a
10   first predetermined address;
        storing a source MAC address of said detected first
data unit;
        forwarding said detected first data unit onto a
plurality of external communication ports;
15   monitoring said plurality of external communication
ports to detect a second data unit having a destination
address matching said first predetermined address received
at a respective one of said plurality of external
communication ports;
20   comparing a source MAC address of said second detected
data unit to said stored source MAC address; and
        in the event that said source MAC address of said
second detected data unit matches said stored source MAC
address, disabling operation of said respective one of said
25   plurality of external communication ports at which said
second detected unit was received.

2. The method of claim 1, wherein said predetermined
destination address is a media access control layer bridge
30   multicast address.

3. The method of claim 1, further comprising discarding said detected second data unit without any forwarding of said detected second data unit over any of said plurality of external communication ports.

4. The method of claim 1, further comprising sending a message to a network management entity indicating that said one of said plurality of external communication ports has been disabled.

5. The method of claim 4, wherein said sending of said message comprises sending said message to a network management entity within said network hub.

6. The method of claim 1, wherein said detected first data unit and said detected second data unit are bridge protocol data units.

7. The method of claim 1, further comprising periodically clearing said stored copy of said source MAC address of said detected first data unit.

8. The method of claim 1, further comprising:
    monitoring said plurality of external communication ports to detect a data unit of a predetermined type; and
    in the event that a data unit is detected of said predetermined type, disabling a respective one of said plurality of external communication ports at which said detected data unit of said predetermined type was received.

9. The method of claim 8, wherein said step of monitoring said plurality of external communication ports to detect a

data unit of said predetermined type comprises monitoring said plurality of external communication ports to detect a router protocol data unit.

5   10. Apparatus for eliminating loops in a network comprising:
        a bridge type input/output module having a plurality of external communication ports and an intra-hub interface for communicably coupling said module with a switching fabric within a network hub, said input/output module including a
10   controller operable to:
            monitor said intra-hub interface to detect a first data unit having a destination address matching a first predetermined address;
            store a source MAC address of said detected first
15   data unit;
            forward said detected first data unit onto said plurality of external communication ports;
            monitor said plurality of external communication ports to detect a second data unit received at a
20   respective one of said plurality of external communication ports and having a destination address matching said first predetermined address;
            compare a source MAC address of said second detected data unit to said stored source MAC address;
25   and
            in the event that said source MAC address of said second detected data unit matches said stored source MAC address, disable operation of said respective one of said plurality of external communication ports at
30   which said second detected unit was received.

11. The apparatus of claim 10, wherein said predetermined destination address is a media access control layer bridge multicast address.

5   12. The apparatus of claim 10, wherein said bridge type input/output module is further operable to discard said detected second data unit without any forwarding of said detected second data unit over any of said plurality of external communication ports.

10

13. The apparatus of claim 10, wherein said bridge type input/output module is further operable to send a message to a network management entity, said message indicating that said one of said plurality of external communication ports

15   has been disabled.

14. The apparatus of claim 13, wherein said bridge type input/output module is further operable to send said message by sending said message to a network management entity

20   within said network hub.

15. The apparatus of claim 10, wherein said detected first data unit and said detected second data unit are bridge protocol data units.

25

16. The apparatus of claim 10, wherein said bridge type input/output module is further operable to periodically clear said stored copy of said source MAC address of said detected first data unit.

30

17. The apparatus of claim 10, wherein said bridge type input/output module is further operable to:

monitor said plurality of external communication ports
to detect a data unit of a predetermined type; and

in the event that a data unit is detected of said
predetermined type, disable a respective one of said
5   plurality of external communication ports at which said
detected data unit of said predetermined type was received.

18. The apparatus of claim 17, wherein said bridge type
input/output module is further operable to monitor said
10   plurality of external communication ports to detect a data
unit of said predetermined type by monitoring said plurality
of external communication ports to detect a router protocol
data unit.

15   19. A system for preventing bridge loops in a network
topology, comprising:

a switching fabric installed in a network hub, said
switching fabric operable to forward data units among a
plurality of input/output modules also installed in said
20   network hub;

a spanning tree protocol controller installed within
said switching fabric, said spanning tree protocol
controller operable to forward bridge protocol data units on
an intra-hub communication path;
25   at least one bridge type input/output module installed
in said network hub, said bridge type input/output module
operable to

monitor said intra-hub communication path of said
network hub to detect a first one of said bridge
30   protocol data units transmitted by said switching
fabric,

store a source MAC address of said detected first
data unit,

forward said detected first data unit onto a
plurality of external communication ports of said
5   bridge type input/output module,

monitor said plurality of external communication
ports to detect a second data unit having a destination
address matching said first predetermined address
received at a respective one of said plurality of
10   external communication ports,

compare a source MAC address of said second
detected data unit to said stored source MAC address,
and

in the event that said source MAC address of said
15   second detected data unit matches said stored source
MAC address, disabling operation of said respective one
of said plurality of external communication ports at
which said second detected unit was received.

20   20. The system of claim 19, wherein said predetermined
destination address is a media access control layer bridge
multicast address.

21. The system of claim 19, wherein said at least one bridge
25   type input/output module installed in said network hub is
further operable to discard said detected second data unit
without any forwarding of said detected second data unit
over any of said plurality of external communication ports.

30   22. The system of claim 19, wherein said at least one bridge
type input/output module installed in said network hub is
further operable to send a message to a network management

entity indicating that said one of said plurality of external communication ports has been disabled.

23. The system of claim 22, wherein said at least one bridge type input/output module installed in said network hub is operable to send said message by sending said message to a network management entity within said network hub.

24. The system of claim 19, wherein said detected first data unit and said detected second data unit are bridge protocol data units.

25. The system of claim 19, wherein said at least one bridge type input/output module installed in said network hub is further operable to periodically clear said stored copy of said source MAC address of said detected first data unit.

26. The system of claim 19, wherein said at least one bridge type input/output module installed in said network hub is further operable to:

    monitor said plurality of external communication ports to detect a data unit of a predetermined type; and

    in the event that a data unit is detected of said predetermined type, disable a respective one of said plurality of external communication ports at which said detected data unit of said predetermined type was received.

27. The system of claim 26, wherein said at least one bridge type input/output module installed in said network hub is operable to monitor said plurality of external communication ports to detect a data unit of said predetermined type

comprises by monitoring said plurality of external communication ports to detect a router protocol data unit.